REMARKS

[0001] Claims 1 and 39-52, and 54 remain in the case and stand rejected. The Office Action objected to Claims 1 and 39. The Office Action rejected Claims 1 and 39-52, and 54 under 35 U.S.C. § 112, second paragraph as being indefinite. The Office Action rejected Claims 1 and 39-52, and 54 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,795,555 to Parisien et al. (hereinafter "Parisien") in further view of European Patent Application No. 0999673 to Mamros et al. (hereinafter "Mamros").

AMENDMENTS TO THE CLAIMS

[0002] Applicants have amended Claims 1, 39, 44, and 50 to clarify embodiments of the invention. The Applicants have cancelled Claims 40, 45, and 46 because the limitations of these claims have been incorporated into the preceding independent claim by amendment. Applicants have amended Claims 41, 42, 47, and 51 for consistency with the other claim amendments/ cancellations and have amended Claim 43 for grammar. The amendments are fully supported by the Specification, Claims, and Drawings and will be discussed in relation to the corresponding rejection. No new matter has been added.

REJECTION OF CLAIMS 1, 39-52, AND 54 UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

[0003] The Office Action rejected Claims 1 and 39-52, and 54 under 35 U.S.C. § 112, second paragraph as being indefinite. Specifically, the Office Action argues that the relationship between idleness and the heartbeat is too "loosely coupled." Applicants have amended Claims 1, 39, 44, and 50 and removed reference to the heartbeat. As agreed during the telephone interview, the amendments overcome the rejection under 112. Consequently, the Applicants respectfully request that this rejection be withdrawn.

OBJECTION TO CLAIMS 1 AND 39

[0004] The Office Action objected to Claims 1 and 39 for informalities. Specifically, the Office Action stated these claims recite a processor and a memory twice. Applicants have amended Claims 1 and 39 to remove one instance of the processor and memory. Consequently, the Applicants respectfully request that these objections be withdrawn.

REJECTION OF CLAIMS 1, 39-52, AND 54 UNDER 35 U.S.C. §103(a)

[0005] The Office Action rejected Claims 1, 39-52, and 54 under 35 U.S.C. § 103(a) as being unpatentable over Parisien in further view of Mamros. The Applicants respectfully traverse this rejection.

[0006] The Examiner bears the initial burden of establishing a *prima facie* case of obviousness. MPEP at § 2142. The prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP at § 2142. Furthermore, the factual inquiries for determining obviousness are summarized as follows:

1. Determine the scope and content of the prior art.
2. Determine the differences between the prior art and the claims at issue.
3. Resolve the level of ordinary skill in the pertinent art.
4. Consider objective evidence present in the application indicative of obviousness or nonobviousness.

Graham v. John Deere Co., 383 US 1, 148 USPQ 459 (1966).

[0007] Obviousness may also be rebutted by showing that "the art, in any material respect, teaches away from the claimed invention." MPEP at § 2144.05.III. "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of

course depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant." *United States v. Adams*, 383 U.S. 39, 52, 148 USPQ 479, 484 (1966).

[0008] Applicants assert that the Office Action fails to establish a *prima facie* case of obviousness, first because not all elements of the amended claims are taught or suggested in the art of record, second, because the factual inquiry of Graham weighs in favor of nonobviousness, and third, because a reference teaches away from the claimed invention.

SCOPE AND CONTENT OF THE ART

[0009] Parisien seems to describe an encryption scheme for use with terminal devices. Parisien, Abstract. Specifically, Parisien appears to be directed at reducing delays and use of resources to calculate encryption keys by generating these keys before the keys are needed. *Id.*, col. 4, l. 20. Parisien states "The method of the present invention avoids unnecessary delay by **pre-establishing** a set of symmetric encryption keys (i.e. "session" keys) for **immediate use** by network elements such as calling party CPE 10 and called party CPE 12." *Id.* at col. 4, ll. 20-24 (emphasis added). Parisien appears to generate a set or "chain" of encryption keys before the keys are needed (one generated key seems to be used to encrypt the next key, thus forming a chain). *Id.*, *id.* at ll. 33-36, 64. Although one key is used to encrypt the next, most of the keys in the chain appear to be pre-generated. *See id.* at col. 5, l. 48 (keys K1-K3 are initially generated, while K4 is generated later).

[0010] Parisien appears to describe periodic key refreshes **during** system idle times to "break the chain." *Id.* at col 4, ll. 37-38. Regarding the refreshing of these keys, Parisien states "Such refreshing of keys should preferably take place once every 24 hours." *Id.* at col. 5, l. 33.

[0011] Mamros appears to describe a system to determine the reachability of a remote computer over a telephone line. Mamros, Abstract. Mamros also appears to describe a protected keep alive message transmitted between computers that is not a rekey request. *Id.*

DIFFERENCES BETWEEN THE PRIOR ART AND THE CLAIMS AT ISSUE

[0012] **Claim 1**:The Applicants respectfully submit that amended Claim 1 as amended recites features not taught or suggested in Parisien and Mamros. Claim 1 as amended states:

> 1. Currently Amended) A method for facilitating secure data communications using a secret key for encrypting data flowing between first computing node comprising a processor and a memory and second computing node ~~comprising a processor and a memory~~ over a communications link, the method comprising:
> determining that the communications link has been idle for at least a predetermined period of time ~~is idle~~, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data transmission within the at least a predetermined period of time ~~in response to detecting that a heartbeat flowed across the communications link~~;
> determining that there is data to flow over the idle communications link between the first computing node and the second computing node; and
> generating a new secret key **on demand** exclusively in response ~~responsive~~ to determining that there is data to flow over the ~~previously~~ idle communications link **and** in response to determining that the communication link ~~is~~ has been idle for at least the predetermined period of time, ~~initiating generation of a new secret key,~~ the new secret key for encrypting data sent between the first computing node and the second computing node over the communications link.

Claim 1 as amended (strikeout removed for clarity, emphasis added). The amendments to Claim 1 find support in Claim 40 now cancelled and paragraphs 16 and 28 of the Specification. Claim 1 has also been amended to clarify that the idle communication link has "no secure data transmission within the at least a predetermined period of time." This amendment finds support in at least paragraphs 19 and 70. Paragraph 70 states that heartbeats do not need to be encrypted. Therefore, a heartbeat does not constitute "secure data transmission." Therefore, the amendment clarifies that a communication link may be considered idle, but still transmit heartbeat messages

because a heartbeat message is not secure data transmission. Therefore, no new matter has been added.

[0013] The art of record fails to teach "generating a new secret key on demand exclusively in response to determining that there is data to flow over the idle communications link and in response to determining that the communication link has been idle for at least the predetermined period of time."

[0014] Parisien is directed at reducing the time required when refreshing or calculating keys. Parisien "avoids unnecessary delay by **pre-establishing** a set of symmetric encryption keys (i.e. "session" keys) for **immediate use** by network elements such as calling party CPE." *Id.* at col. 4, ll. 20-24 (emphasis added). Therefore, the goals of Parisien are the *exact opposite* of the claimed invention. Parisien sets up the encryption keys before data is ready to be transmitted so that when data becomes ready, the data can easily be encrypted and sent without waiting for generation of encryption keys. In contrast, the claimed invention refreshes encryption keys *when data is ready* to be transmitted not ahead of time as in Parisien. Additionally, because Parisien generates keys before they are used, Parisien fails to teach "generating a new secret key **on demand**."

[0015] Furthermore, Parisien appears to describe periodic key refreshes **during** system idle times to "break the chain." Parisien at col 4, ll. 37-38. The language "during system idle times" indicates that the system is idle before and after the refresh, not when "determining that there is data to flow over the previously idle communications link" as in amended Claim 1. Furthermore, Parisien fails to describe a key refresh caused by having data ready to transmit. In fact, Parisien seems to indicate that the key refreshing is an automatic process conducted regardless of whether data is available for transmission and also key refreshing appears to be at a set time. Regarding the refreshing of these keys, Parisien states "Such refreshing of keys should **preferably** take place **once every 24** hours." *Id.* at col. 5, l. 33.

[0016] Mamros fails to teach or describe the claim elements discussed above found lacking in Parisien. Furthermore, Mamros, which describes renegotiating when a certain amount

of data has been transferred or when a certain amount of time has elapsed, also fails to teach the limitations of Claim 1. Mamros, ¶ 32.

[0017] By renegotiating only when data is available to send, as in the claimed invention, system overhead and resources are saved. For example, a communications link that is idle for a long period of time will continually renegotiate the secure key in a prior art system that performs that action on a timed basis.

[0018] Because Parisien and Mamros fail to teach the elements of Claim 1, Parisien and Mamros are non-obvious in view of Claim 1 as amended. Consequently, Applicants respectfully request that the rejection of Claim 1 under 35 U.S.C. §103(a) be withdrawn. Applicants respectfully assert that amended Claims 39 and 44 are also not obvious over Parisien and Mamros for at least the same reasons as amended Claim 1. Furthermore, Claim 44 has an additional limitation of a "byte measurer" to refresh the key when a threshold amount of data has been transmitted. Therefore, Applicants respectfully request that the rejection of Claims 39 and 44 under 35 U.S.C. §103 (a) be likewise withdrawn. Furthermore, dependent Claims 41-43 and 47-49 are also allowable for depending on allowable independent claims.

[0019] **Claim 50**:The Applicants respectfully submit that amended Claim 50 as amended recites features not taught or suggested in Parisien and Mamros. Claim 50 as amended states:

> 50. (A program product comprising a computer readable storage media embodying program instructions executed by a computer to facilitate secure data communications with a remote system by using a secret key for encrypting data flowing between the computer and the remote system over a communications link by:
> determining that the communications link <u>has been idle for at least a predetermined period of time, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data communication traffic within the at least a predetermined period of time</u>;
> sending a heartbeat message to the remote system only if it is determined that the link has been idle for at least a predetermined period of time and that there is no data available for flow over the communications link;

monitoring the communications link for receipt of an acknowledgement from the remote system;
receiving the acknowledgement from the remote system within a predetermined period of time;
determining that data is available for flow over the idle communications link from the computer to the remote system;
detecting that a heartbeat flowed across the idle communications link; and
generating a new secret key on demand exclusively in response to a determination that data is available for flow over the idle communications link, detecting that a heartbeat flowed across the idle communications link, and receiving the acknowledgement from the remote system within the predetermined period of time, the new secret key for use in encoding at least part of the available data before the available data flows onto the communications link, such that generation of a new secret key exclusively occurs when data is available for flow over the idle communications link.

Claim 50 as amended (strikeout removed for clarity, emphasis added). The amendments to Claim 50 find support in paragraphs 16, 28, and 68 of the Specification. Therefore, no new matter has been added.

[0020] The art of record fails to teach "generating a new secret key on demand exclusively in response to a determination that data is available for flow over the idle communications link, detecting that a heartbeat flowed across the idle communications link, and receiving the acknowledgement from the remote system within the predetermined period of time."

[0021] Mamros seems to describe "keep alive" messages, but Mamros fails to teach regenerating a secure key in response to one of these "keep alive" messages having been transmitted. Furthermore, Parisien fails to teach heartbeats or a determination that the last transmission was a heart beat as opposed to a secure data transmission. Beneficially, renegotiating after a heartbeat has been issued provides extra security in case an attacker has managed to hack into the secret key.

[0022] Because Parisien and Mamros fail to teach the elements of Claim 50 as amended, Parisien and Mamros are sufficiently different from Claim 50 as amended and amended Claim 50

is not obvious over these references. Consequently, Applicants respectfully request that the rejection of Claim 50 under 35 U.S.C. §103(a) be withdrawn. Furthermore, dependent Claims 51, 52 and 54 are also allowable for depending on allowable independent claims.

LEVEL OF ORDINARY SKILL IN THE ART

[0023] As stated in the MPEP, the "hypothetical 'person having ordinary skill in the art' to which the claimed subject matter pertains would, of necessity have the capability of understanding the scientific and engineering principles applicable to the pertinent art." Ex parte Hiyamizu, 10 USPQ2d 1393, 1394 (Bd. Pat. App. & Inter. 1988) (The Board disagreed with the examiner's definition of one of ordinary skill in the art (a doctorate level engineer or scientist working at least 40 hours per week in semiconductor research or development), finding that the hypothetical person is not definable by way of credentials, and that the evidence in the application did not support the conclusion that such a person would require a doctorate or equivalent knowledge in science or engineering.); MPEP 2141.03.

[0024] Therefore, Applicants respectfully submit that a person of skill in the art of the present invention is a person that has the capability of understanding the scientific and engineering principles applicable to data encryption and generating encryption keys.

OBJECTIVE EVIDENCE OF NON-OBVIOUSNESS

[0025] Applicants respectfully assert that the invention presented in the pending claims is sufficiently distinct from the prior art taught in Parisien and Mamros. The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. *In re Keler*, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). As previously noted, none of the prior references suggest renegotiating a secret key in response to both a communications link that has been idle for a predetermined period of time and data available to send over the communications link. Parisien is directed at having predetermined keys to use so that keys don't need to be refreshed when data is available to send – the exact opposite of the claimed invention.

[0026] The question is: would one in art when presented with Parisien and Mamros consider modifying one or the other to renegotiating only when the communications link is idle and data is available to send. Applicants submit that one in the art would not make such a leap. Applicants submit that the features of their invention represent a nonobvious improvement over the art. Therefore, Applicants submit that the evidence weighs in favor of nonobviousness.

TEACHING AWAY

[0027] As stated above, Parisien is directed at reducing the time required when refreshing or calculating keys. Parisien "avoids unnecessary delay by **pre-establishing** a set of symmetric encryption keys (i.e. "session" keys) for **immediate use** by network elements such as calling party CPE." *Id.* at col. 4, ll. 20-24 (emphasis added). Therefore, the goals of Parisien are the *exact opposite* of the claimed invention and Parisien teaches away from refreshing keys when data is ready to be transmitted. Parisien sets up the encryption keys before data is ready to be transmitted so that when data becomes ready, the data can easily be encrypted and sent. The claimed invention refreshes encryption keys *when data is ready* to be transmitted.

CONCLUSION

In view of the foregoing, Applicants submit that the application is in condition for immediate allowance. In the event any questions or issues remain that can be resolved with a supplemental phone call, the Examiner is respectfully requested to initiate a telephone conference with the undersigned.

Respectfully submitted,

Date: July 10, 2009

/ David J. McKenzie /

David J. McKenzie
Reg. No. 46,919
Attorney for Applicants

8 East Broadway, Suite 600
Salt Lake City, UT 84111
Telephone (801) 994-4646
Fax (801) 531-1929